FortiClient EMS - Release Notes

VERSION 1.0.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

October 16, 2015

FortiClient EMS 1.0.0 Release Notes

04-100-290940-20151016

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-10-09	Initial release.
2015-10-16	Additional information added to Endpoints managed by FortiGate Devices.

Introduction

FortiClient Enterprise Management Server (EMS) is a system intended to be used to manage large installations of FortiClient. It uses the same Endpoint Control protocol that was introduced in FortiOS 5.0 and enhanced in FortiOS 5.2. Like FortiOS, EMS supports all FortiClient platforms: Microsoft Windows, Mac OS X, Android OS and Apple iOS. FortiClient EMS does not require a Fortinet device. It runs on a Microsoft Windows server. End users with multiple FortiClient installations could choose to use a FortiGate or the EMS to manage their installations.

This document provides the following information for FortiClient EMS 1.0.0 build 0018:

For more information about FortiClient EMS, see the *FortiClient EMS Administration Guide*.

Supported platforms

The EMS server can be installed on any of the following platforms:

- Microsoft Windows Server 2012, 2012 R2
- Microsoft Windows Server 2008 R2

System Requirements

The minimum system requirement is as follows.

- 2.0 GHz 64-bit processor, dual core (or two virtual CPUs)
- 2 GB RAM
- 5 GB free hard disk
- Gigabit (10/100/1000baseT) Ethernet adapter
- Internet access

See also the subsection: Management Capacity in the Main Features section of this document for more details.

Internet access is required during installation. This becomes optional once installation is completed. The EMS uses access to the internet to obtain information about FortiGuard engine and signature updates.

Endpoint Requirements

The following FortiClient platforms are supported:

- FortiClient for Microsoft Windows
- FortiClient for Mac OS X

- FortiClient for Android OS
- FortiClient for iOS

The FortiClient version should be 5.2.4 or newer.

FortiClient is supported on multiple Microsoft Windows and Mac OS X platforms. The EMS supports all such platforms as endpoints.

Licensing

EMS offers a trial license for 60 days from the date of installation with 20,000 seats. See Trial license in the Main Features section in this document for details.

Each FortiClient registered to the EMS uses a single license, while registered. Licenses are available in multiples of 100 seats, with a minimum of 100.

The EMS may be used alone or alongside a FortiGate. The FortiGate integration allows the administrator to configure Network Access Control (NAC) for the network. When used together, both the EMS and the FortiGate require licenses for the number of clients that will be registered or monitored.

Main features

The core features of the FortiClient EMS 1.0.0 include the following:

FortiClient Endpoint Registration Server

FortiClient end users can register to the EMS. The process is similar to registering to a FortiGate. The end user provides the IP address or Fully Qualified Domain Name (FQDN) of the EMS in the Endpoint Control registration box in FortiClient. The EMS shows basic information about the registered endpoint, including:

- Computer name
- User name
- IP address
- Registration status (on-net, off-net, offline, etc.)
- Operating system
- FortiClient version
- FortiGuard engine and signature update status

Endpoint Profiles

Different FortiClient configurations can be created using an easy to use Web-based Manager, or by harnessing the flexibility provided by the FortiClient XML configuration.

A profile can be assigned to a group of registered endpoints. Profiles can be created, updated or removed. Updated profiles will be pushed to registered users automatically. Users may register at any time to retrieve the latest assigned profile. A default profile is assigned to registered endpoints that do not have a designated profile.

The Basic Configuration offers the most commonly used configuration options. A *show advanced option* button is provided within the Basic view. This exposes more options in the Basic view, allowing the administrator to modify most FortiClient options without manually editing the XML configuration.

Endpoints in Active Directory Domain Services

For organizations that use Active Directory Domain Services (AD server) to manage computers, there is an easy to use the interface to import computers into the EMS. Computers that join the AD server will be listed in the EMS, preserving the AD Organizational Unit (OU) structure. The EMS presents basic information about each computer as retrieved from the AD server, including:

- Computer name
- Organizational unit (and structure)
- Operating system

A group of computers imported into the EMS may be assigned any endpoint profile. If any of the endpoints in the domain register to the EMS, additional information become available, such as:

- User name
- IP address
- Registration status

Endpoints in Workgroups

The EMS will automatically detect any computer running Microsoft Windows that is running the Computer Browser Service within the same local network. These computers are listed in the EMS, with similar details as endpoints discovered from an AD server. The name of the workgroup replaces information about the organizational unit from the AD server.

Scanning local workgroups is disabled by default. Go to the *View* > *Settings* menu item to enable it.

Remote Endpoints

Not all computers within an organization will show in the Computer Browser Service. For companies that do not already use an AD server to manage computers, users can join the EMS by registering to it directly. This also works for devices that do not support the AD server or Computer Browser Service. Remote users can register to the EMS by providing the IP address or FQDN of the EMS to FortiClient.

Custom Groups

Computer endpoints may be added into the EMS using multiple methods:

- Importing from an Active Directory (AD) server
- Discovering computers from the local network
- Registering manually from the installed FortiClient

Endpoints imported from an AD server may already have a structured organization or containers. Similarly, computers discovered from the local network may already belong to an intended workgroup. In the event that these pre-existing structures do not match present or future needs, new custom groups can be created in the EMS. Endpoints can then be moved into the custom groups as required.

An organizational structure can be represented in the EMS using nested custom groups. The EMS administrator can apply FortiClient profiles to groups at various levels. Nested groups with unassigned profiles inherit profiles from their immediate parent group.

Dashboard Summary

Managed endpoints' activities are summarized in the EMS dashboard page on the landing page after signing into the EMS GUI. Pie charts are used to show the number of managed clients, online/offline status of clients, and on-

net/off-net status of clients. A bar chart shows a summary of warnings, inactivity, and protection status for managed endpoints.

The sections in each of the charts are live links. Any section of the pie or bar charts may be clicked to find all matching records reflected in the summary.

Antivirus Scan Results

The EMS will show the current antivirus (AV) scanning in the GUI. Statuses are provided for each managed client that is online.

FortiClient runs scheduled AV scans by default. The EMS administrator may include AV scanning schedules in endpoint profiles. The administrator may also request a one-time AV scan from the EMS GUI. For each of these scanning requests, the EMS displays the current status.

Alert Messages

The EMS generates various notifications for the administrator. These are available in the EMS GUI by selecting the *Alert Icon* (a bell). Examples of events that generate alerts include:

- New version of FortiClient is available
- FortiClient deployment failed
- Unable to check for signature updates
- Error encountered while downloading AD server entries or while checking for local computers

A red label is associated with the *Alert* icon when new notifications are available or received. It is cleared once the alert has been viewed.

Trial License

FortiClient EMS provides a trial period of 60 days from the time of installation (with 20,000 seats). These licenses will allow EMS administrators to evaluate the product's full feature set with a sufficiently large number of endpoints as desired. Once the trial license expires, the default license will revert to 10 seats.

A valid product license may be applied any time during or after the trial period. The number of licenses required is based on the number of clients that are deployed or registered by the EMS: one license is required for each client that is deployed or managed.

FortiClient Deployment

The EMS can be used to deploy and install FortiClient on computers running Microsoft Windows. The computers must have joined an AD server that has been added into the EMS. The deployed FortiClient installer may be repackaged to install only some of FortiClient's features. FortiClient can automatically register to the EMS once installation is completed. The AD server requires some simple group policy changes to prepare it for FortiClient deployment.

Endpoints managed by FortiGate Devices

This feature requires your FortiGate to be running FortiOS 5.4.0 or later.

The EMS can deploy FortiClient to endpoints that are, and will continue to be, managed by a FortiGate. FortiClient profiles can be loaded from a FortiGate to the EMS, and then distributed to new endpoints that are registered to the FortiGate.

The FortiGate, in this case, may be configured to enforce Network Access Control (NAC). FortiClient needs to register to the FortiGate to satisfy NAC requirements. FortiClient will continue to send notifications to the EMS. The administrator can monitor FortiClient registration status from the EMS.

Management Capacity

The EMS is intended for use by enterprises. It has the capacity to manage a large number of endpoints. The following are suggested EMS host system hardware configurations, depending on the number of endpoints being managed.

Suggested minimum EMS system hardware

Max number of managed endpoints	Number of Virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
10,000	2	4	default
20,000	4	8	default
30,000	4	8	120 seconds
40,000	4	8	120 seconds
50,000	4	8	120 seconds

For the purpose of this table, an Intel i5 processor with two cores and two threads per core will be considered to have 4 virtual CPUs. An Intel i3 processor with two cores and one thread per core has two virtual CPUs.

Each registered FortiClient sends a short keep alive message to the EMS at a regular interval. The keep alive message carries various update information from the client to the EMS. If a modification or change is made on the EMS, it sends it to the clients in the keep alive reply.

The default keep alive interval in FortiOS 5.2 is 120 seconds. It is 60 seconds by default in the EMS. To change the keep alive interval, select on the EMS GUI the *View* > *Settings* menu item, and click the Client Settings tab.

Installation

Installing the EMS

FortiClient EMS is available for download from each of the following:

- Fortinet Support website
- Contacting a sales representative

Software Dependencies

The EMS requires Microsoft SQL Server 2014 Express to be installed on the server. The EMS installer will automatically install it if it is not already installed. Microsoft SQL Server Express has its own software dependencies. Some of these must be downloaded during the EMS installation. For this reason, access to the internet is required during installation.

The setup progress bar may appear to freeze for about 15 minutes while installing Microsoft SQL Server 2014 Express. The full EMS installation can take about 20 minutes to complete

Uninstalling the EMS

Use the *Programs and Features* pane of the Control Panel in Microsoft Windows to uninstall the EMS.

The EMS installs the following dependencies. If they are not being used by other applications on the same computer, they can be uninstalled manually after the EMS has been removed.

- Microsoft ODBC Driver 11 for SQL Server
- Microsoft SQL Server 2008 Setup Support Files
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server 2014 (64-bit)
- Microsoft SQL Server 2014 Setup (English)
- Microsoft SQL Server 2014 Transact-SQL ScriptDom
- Microsoft Visual C++ 2010 x64 Redistributable – 10.0
- Microsoft Visual C++ 2010 x86 Redistributable – 10.0
- Microsoft Visual C++ 2013 x86 Redistributable – 12.0
- Microsoft VSS Writer for SQL Server 2014
- SQL Server Browser for SQL Server 2014

The EMS creates an application state in a local Microsoft SQL Server Express database. Uninstalling the EMS permanently removes this state.

Connecting to the EMS console

Following a successful installation, the EMS will create a desktop icon that can be used to open the EMS console. The console is also accessible through an appropriate web browser.

Default user

As with other Fortinet products, a default user named admin, with no password, is created at the time of installation. The password should be added after the installation is complete.

Ports and Firewalls

EMS services listen on the following ports:

Port	EMS Component	Notes
8013	Endpoint Registration	The EMS listens on this port for FortiClient registrations. This is the default in FortiOS as well. The port can be changed in the EMS settings page. The traffic exchanged between FortiClient and the EMS on this port is encrypted using SSL.
10443	EMS Console	Any FortiClient installers created will be available for download using the HTTPS port 10443.
443	Apache Server	A modern browser can be used to connect to the EMS console using HTTPS.

Known Issues

The following issues have been identified in version 1.0.0. For inquires about a particular bug or to report a bug,please contact Customer Service & Support.

Bug ID	Description
262374	FortiAnalyzer may not support FortiClient log upload if it is registered to EMS.
288121	Add option to configure *Vulnerability Scan* feature in Endpoint Profile GUI
290011	Error message may not appear write permission is denied on folder `FortiEMSInstaller`.
291532	Reboot prompt may appear when installing the same package with EMS.
292695	*Auto-connect VPN* may auto connect when EMS pushes any new profile.
292818	EMS scan request may not work with an offline device.